

**Política RA
de la
Fundació per a la
Universitat Oberta de Catalunya**

v: 1.1.0

Barcelona, 24 de Febrero 2009

Índice de contenido

1. Presentación	4
2. Operadores de la RA	4
3. Aprobación de solicitudes de certificado.	4
3.1. Autenticación del solicitante	4
3.1.1. Reunión cara a cara	4
3.1.1.1 Detalles de la reunión	4
3.1.1.2 Documentos Aceptados	5
3.1.1.3 Documentación archivada	5
3.1.3 Otros métodos	5
3.2 Verificación del solicitante	5
3.2.1 Descripción del procedimiento para certificado de personas físicas	5
3.2.1.1 Verificación en la reunión cara a cara	5
3.2.2 Descripción del procedimiento para certificado de servidor	6
3.2.3 Documentación archivada	6
4. Política de revocaciones	7
4.1 Solicitud de revocaciones por iniciativa de la RA	7
4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado	7
4.3 Solicitud de revocación cuando un usuario abandona la institución	7

Historia:

25/11/2008	Sergio Pérez	Redacción del borrador.
09/02/2009	Sergio Pérez	Revisión.
10/02/2009	Sergio Pérez	Revisión y formato. Primera versión.
24/02/2009	Sergio Pérez	Supresión identificación mediante certificado digital. Actualización de documento de identidad aceptado (3.1.1.2).
25/02/2009	Sergio Pérez	Revisión.

1. Presentación

Se presenta en este documento la política de la Autoridad de Registro, en adelante RA, de la Fundació per a la Universitat Oberta de Catalunya, en adelante UOC, con el objetivo de establecer el proceso de concesión de certificados pkIRISGrid en la UOC.

La UOC, con sede central en Barcelona, es una universidad no presencial con estudios homologados.

La UOC está afiliada a RedIRIS desde 1995, y en la actualidad trabajan en él más de 100 investigadores que participan activamente en proyectos relacionados con todos los aspectos de la sociedad de la información.

2. Operadores de la RA

Los operadores de la RA de la UOC han de ser personal UOC, pertenecientes al área de Recursos Humanos, con contrato estable, con más de dos años de experiencia, y con conocimientos medios de informática.

Todos los operadores de la RA de la UOC deben haber sido formados para su labor por personal de pkIRISGrid u otros operadores de la RA de la UOC.

Cuándo un operador deja de serlo o abandona la UOC, los restantes operadores cambian la contraseña de operador.

3. Aprobación de solicitudes de certificado.

La RA de la UOC aprueba solicitudes de certificado tanto de usuario como de servidor para sus investigadores. El proceso debe realizarse mediante una reunión cara a cara con el solicitante.

3.1. Autenticación del solicitante

El proceso de autenticación del solicitante de certificados será el mismo tanto para solicitudes de certificado de usuario como de servidor.

3.1.1. Reunión cara a cara

La forma básica de autenticación del solicitante de certificado es la reunión cara a cara. Una vez que ha solicitado su certificado desde su navegador y haya sido contactado por un operador de RA, el solicitante se desplazará a la RA de la UOC, presentará su documento de identidad (DNI o pasaporte), y comunicará su pin al operador. Éste procederá a generar la documentación descrita más abajo, archivarla, y aprobará la solicitud.

Una vez aprobada, el operador de la RA enviará la solicitud a la CA en el plazo de dos días laborables.

3.1.1.1 Detalles de la reunión

La RA de la UOC está situada en la sede central (Av. Tibidabo 39-43, Barcelona). El horario de apertura se indicará en la web del mismo. El solicitante dispondrá de un plazo de 7 días

hábiles para acudir a la reunión cara a cara después de que el operador de la RA haya contactado con él, si bien los días pueden variar dependiendo de la disponibilidad de los operadores.

3.1.1.2 Documentos Aceptados

Los ciudadanos españoles podrán presentar cualquiera de los documentos de identidad aceptados por la legislación española (DNI, o pasaporte). El carné de UOC no será aceptado al no tratarse de un documento aceptado por la legislación española.

Los ciudadanos no españoles tanto comunitarios como no comunitarios podrán presentar el pasaporte.

3.1.1.3 Documentación archivada

En el proceso de autenticación del solicitante el operador de la RA contrastará los datos de la solicitud del certificado con los de el documento de identidad presentado. Si los datos son correctos, se fotocopiará el documento, y se guardará, junto con los datos y la fecha del certificado para futuras auditorías.

3.1.3 Otros métodos

No aplicable.

3.2 Verificación del solicitante

Tras la autenticación del solicitante, se ha de verificar la autoridad de éste para solicitarlo antes de aprobar la solicitud. En todos los casos se verificará la dirección de correo electrónico.

3.2.1 Descripción del procedimiento para certificado de personas físicas

3.2.1.1 Verificación en la reunión cara a cara

El solicitante presentará en la reunión cara a cara con la RA su carné de UOC. El carné se fotocopiará y se guardará junto a las fotocopias de los documentos que se hicieron en la fase de autenticación.

Se verificará el correo electrónico pidiendo al solicitante que responda al correo con el que se le cita a la reunión cara a cara, antes de acudir a ella.

En caso de que el solicitante sea personal visitante de la UOC deberá presentar un documento, firmado por el director de la institución, que le acredite como tal.

3.2.2 Descripción del procedimiento para certificado de servidor

La persona solicitante deberá presentar un documento firmado por la Persona de Enlace con RedIRIS¹ (PER) de la UOC y el responsable de la máquina que autoricen al solicitante a pedir un certificado de servidor. Este documento o documentos se guardarán junto con los documentos generados en la fase de autenticación.

3.2.3 Documentación archivada

Descrito en los apartados 3.2.1 y 3.2.2.

¹ Actualmente el PER es el vicerrector de Sistemas de Información.

4. Política de revocaciones

Las siguientes subsecciones describen en qué casos la RA puede solicitar la revocación de un certificado. En todas las solicitudes de revocación se generará un informe con los datos del operador que la solicitó, la circunstancias que provocaron la solicitud, la fecha, y otros documentos justifiquen dicha decisión, como los datos de autenticación en caso de iniciativa del usuario, o informes que muestren el mal uso de los certificados.

4.1 Solicitud de revocaciones por iniciativa de la RA

La RA solicitará la revocación de un certificado por iniciativa propia cuando:

- En el caso de un usuario:
 - Está usando los servicios a los que tiene acceso con su certificado para usos ajenos a la UOC o de forma indebida.
 - Se detecta que el usuario tiene instalado el certificado en un ordenador al que tienen acceso varias personas.
 - Se detecta un robo de la clave pública.
 - El usuario comparte su certificado o le da otros usos incompatibles con el objetivo de un certificado digital.
 - El usuario deja de tener permiso de la institución que lo avaló para usar el certificado.
 - Otros usos del certificado que el operador estime incorrectos o que puedan dañar la imagen o la reputación de pkIRISGrid o de la UOC.
- En el caso de certificados de servicio/servidor:
 - Se detecta que la clave privada del servidor se ha visto comprometida.
 - Se detecta que el certificado está instalado en varias máquinas, sin ser un sistema de alta disponibilidad.
 - El servicio que ofrecía el servidor para el que se pidió el certificado deja de ofrecerse.

4.2 Solicitud de revocaciones por iniciativa del usuario del Certificado

La RA solicitará la revocación de un certificado a petición del usuario siempre que éste se autentique (de acuerdo con la subsección 3.1 sobre autenticación), o lo solicite por teléfono comunicando el pin del certificado.

4.3 Solicitud de revocación cuando un usuario abandona la institución

La secretaría de recursos humanos de la UOC informa a la RA siempre que hay una baja de personal, ya sea local o visitante. La RA procede entonces a emitir la solicitud de revocación de certificado.